Benjamin Heikali (SBN 307466)
E-mail: bheikali@faruqilaw.com
Joshua Nassir (SBN 318344)
E-mail: jnassir@faruqilaw.com
**FARUQI & FARUQI, LLP**
10866 Wilshire Boulevard, Suite 1470
Los Angeles, CA 90024
Telephone: (424) 256-2884
Facsimile: (424) 256-2885

*Attorneys for Plaintiffs and the Putative Classes*

[Additional Counsel Listed On Signature Page]

**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF CALIFORNIA**

BELINDA L. FISHER, JAMES SCOTT JEWELL, HOWARD CLARK, AMANDA STEVENS, AND CASEY THAXTON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A.,

Defendants.

Case No.:3:19-cv-4485

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Belinda L. Fisher, James Scott Jewell, Howard Clark, Amanda Stevens, and Casey Thaxton ("Plaintiffs"), by and through their counsel, bring this Class Action Complaint against Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA) ("Defendants") on behalf of themselves and all others similarly situated, and allege upon personal knowledge as to their own actions, and upon information and belief as to counsel's investigations and all other matters, as follows:

## JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs, there are more than 100 putative class members nationwide, and at least one putative class member and Defendants are citizens of different states.

2. This Court has personal jurisdiction over Defendants because Defendants have sufficient minimum contacts in California. Defendants intentionally avails themselves of this jurisdiction by marketing, distributing, and selling their banking and credit card services throughout California, including this District.

3. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims occurred in this District. Specifically, Plaintiff Clark applied for Defendants' credit cards and therefore provided Defendants with his Customer Data in this District.

## PARTIES

### A. Plaintiff

4. Plaintiff Belinda L. Fisher is a resident of Portland, Oregon and was an Oregon resident during the period of the Data Breach. Plaintiff Fisher has applied for three Capital One credit card between 2014 and 2016. In doing so, Plaintiff Fisher has provided Defendants with her Customer Data. On information and belief, Plaintiff Fisher had her Customer Data (defined below) compromised during the Data Breach. If Plaintiff had known that Defendants' data security measures were inadequate to safeguard customers' Customer Data from theft, she would not have applied for

credit cards and provided Defendants with their Customer Data. Plaintiff Fisher has spent approximately two hours in response to the Data Breach, including reviewing her financial accounts, contacting Defendants, and reviewing Defendants' website and press releases.

5. Plaintiff James Scott Jewell is a resident of Tonganoxie, Kansas and was a Kansas resident during the period of the Data Breach. Plaintiff Jewell has applied for a Capital One credit card on or around May 2013. In doing so, Plaintiff Jewell has provided Defendants with his Customer Data. On information and belief, Plaintiff Jewell had his Customer Data compromised during the Data Breach. If Plaintiff Jewell had known that Defendants' data security measures were inadequate to safeguard customers' Customer Data from theft, he would not have applied for credit cards and provided Defendants with their Customer Data. Plaintiff Jewell has spent time in response to the Data Breach, including attempting to find out whether his Customer Data was compromised.

6. Plaintiff Howard Clark is a resident of San Francisco, California and was a California resident during the period of the Data Breach. Plaintiff Clark has applied for Defendants' credit cards on three occasions since 2005, with accounts open on or around July 2015, July 2017, and June 2018. In doing so, Plaintiff Clark has provided Defendants with his Customer Data. On information and belief, Plaintiff Clark had his Customer Data compromised during the Data Breach. If Plaintiff Clark had known that Defendants' data security measures were inadequate to safeguard customers' Customer Data from theft, he would not have applied for credit cards and provided Defendants with their Customer Data.

7. Plaintiff Amanda Stevens is a resident of Yakima, Washington and was a Washington resident during the period of Defendants' Data Breach. In 2017, Plaintiff Stevens has applied for a Capital One credit card, and in doing so, has provided Defendants with her Customer Data. If Plaintiff Stevens had known that Defendants' data security measures were inadequate to safeguard customers' Customer Data from theft, she would not have applied for credit cards and provided Defendants with their Customer Data. On information and belief, Plaintiff Stevens had her Customer Data compromised during the Data Breach.

8. Plaintiff Casey Thaxton is a resident of Yakima, Washington and was a Washington resident during the period of Defendants' Data Breach. In 2017, Plaintiff Thaxton applied for a Capital One credit card, and in doing so, has provided Defendants with her Customer Data. Further, while Plaintiff Thaxton was signing up for his Capital One credit card, he read representations by Defendants that his Customer Data would be protected. If Plaintiff Thaxton had known that Defendants' data security measures were inadequate to safeguard customers' Customer Data from theft, he would not have applied for credit cards and provided Defendants with their Customer Data. On information and belief, Plaintiff Stevens had her Customer Data compromised during the Data Breach.

9. Plaintiffs would not have applied for credit cards and provided Defendants with their Customer Data had Defendants told them that they lacked data security practices to safeguard customers' Customer Data from theft.

10. Plaintiffs suffered actual injury from having their Customer Data compromised and stolen in and as a result of the Data Breach.

11. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Customer Data – a form of intangible property that they entrusted to Defendants that was compromised in and as a result of Defendants' Data Breach.

12. Plaintiffs suffer imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Customer Data being placed in the hands of criminals. Plaintiffs have a continuing interest in ensuring that their private information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

**B. Defendants**

13. Defendant Capital One Financial Corporation is a bank holding company organized and existing under the laws of the state of Delaware with its principal place of business located in McLean, Virginia.

14. Defendant Capital One, N.A. is a wholly owned subsidiary of Defendant Capital One Financial Corporation, and also maintains its principal place of business in McLean, Virginia.

15. Defendant Capital One Bank (USA), N.A. is also a wholly owned subsidiary of Defendant Capital One Financial Corporation, and also maintains its principal place of business in McLean, Virginia.

## STATEMENT OF FACTS

16. Plaintiffs bring this consumer class action against Defendants for their failures to secure and safeguard Plaintiffs' and customers' private information, including their names, phone numbers, bank account numbers, social security numbers, credit scores, email addresses, physical addresses, dates of birth and self-reported incomes ("Customer Data").[1] [2]

17. On July 29, 2019, Defendants announced that the Customer Data of over 100 million U.S. individuals was compromised as a result of a hack by Paige A. Thompson, a former cloud service employee at Amazon (the "Data Breach").[3]

18. The Customer Data was extracted from over 100 million credit "card customers and applicants," making the Data Breach "one of the largest-ever data breaches of a big bank."[4]

19. The hacker was able to extract Customer Data from credit card applications ranging as far back as 2005, meaning Defendants continued to store Plaintiffs' and consumers' sensitive Customer Data on its data systems for approximately 14 years.[5]

20. Notably, this Customer Data was vulnerable even for consumers who applied for a CapitalOne card but ultimately did not make an account.[6]

21. Access to the Customer Data, which was hosted on an Amazon web server, occurred

---

[1] Emily Flitter and Karen Weise, *Capital One Data Breach Affects 100 Million; Woman Charged as Hacker* (July 29, 2019), *available at* https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html (last visited July 30, 2019).

[2] Thomas Franck, *How To Tell If You Were Affected By The Capital One Breach* (July 30, 2019), *available at* https://www.cnbc.com/2019/07/30/how-to-tell-if-you-were-affected-by-the-capital-one-breach.html (last visited July 30, 2019).

[3] Nicole Hong, *Capital One Reports Data Breach Affecting 100 Million Customers, Applicants* (July 29, 2019), *available at* https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355 (last visited July 30, 2019).

[4] *Id.*

[5] Hailey Mensik, *Even If You Never Had A Capital One Card, You Still Could Be Exposed* (July 31, 2019), *available at* https://www.latimes.com/business/story/2019-07-30/even-if-you-never-had-a-capital-one-card-you-still-could-be-exposed (last visited July 31, 2019).

[6] *Id.*

through a misconfigured firewall protecting one the servers storing the Customer Data.[7]

22. The private Customer Data obtained from the Data Breach was compromised due to Defendants' acts and omissions and their failure to properly protect the Customer Data. As Defendants admit, the hacker "was able to exploit a specific configuration *vulnerability* in our infrastructure."[8]

23. According to Amazon, clients such as Defendants "maintain full control" of "configuring access" to the web service.[9] As Amazon states, "[y]ou choose how your content is secured."[10] Defendants have admitted as such after the Data Breach, stating that the hacker "[w]as able to exploit a specific configuration vulnerability in our infrastructure."[11]

24. If Defendants had maintained and implemented proper data-security measures to safeguard Customer Data, deter Ms. Thompson, and detect the breach within a reasonable amount of time, it is more likely than not that the breach would have been prevented, or at the very least, its harm mitigated.

25. Plaintiffs' and Class members' Consumer Data is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Plaintiffs' and Class members' consent to disclose their Customer Data to any unauthorized persons as required by applicable law and industry standards.

26. As a result of the Data Breach, Plaintiffs' and Class members' Customer Data has been exposed to third parties for misuse. The injuries suffered or that will likely be suffered by Plaintiffs and Class members as a direct result of Defendants' Data Breach include:

a. unauthorized charges on their bank accounts;

---

7 https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

8 Mathew Katz, New Capital One Data Breach Affects 100 Million People. Here's The Very Latest (July 29, 2019), *available at* https://www.digitaltrends.com/news/capital-one-data-breach-social-security-bank/ (last visited July 29, 2019)

9 Jason Murdock, *Amazon Refuses Blame For Capital One Data Breach, Says Its Cloud Services Were 'Not Compromised In Any Way'* (July 30, 2019), *available at* https://www.newsweek.com/amazon-capital-one-hack-data-leak-breach-paige-thompson-cybercrime-1451665 (last visited July 30, 2019).

10 *Id.*

11 Capital One Financial Corporation, *Capital One Announces Data Security Incident* (July 29, 2019), *available at* https://www.prnewswire.com/news-releases/capital-one-announces-data-security-incident-300892738.html (last visited July 30, 2019).

b. theft of their personal and financial information;

c. costs associated with the detection, prevention, and mitigation of the unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling accounts, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Customer Data being placed in the hands of third parties for misuse;

g. damages to and diminution in value of their Customer Data entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access to and misuse of their information by others; and

h. continued risk to their Customer Data which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data in their possession.

27. These injuries to the Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Customer Data.

28. Plaintiffs and Class members retain a significant interest in ensuring that their Customer Data, which remains in Defendants' possession, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated customers whose Customer Data was stolen as a result of the Data Breach.

29. Plaintiffs, on behalf of herself and similarly situated consumers, seek to recover damages, equitable relief including injunctive relief to prevent a reoccurrence of the data breach and resulting injury, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

**A. Value of Customer Data On the Cyber Black Market**

30. Stolen private information is a valuable commodity. A "cyber black-market", exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. The private data is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

31. Legitimate organizations and the criminal underground alike recognize the value in private personal data contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it.

32. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[13]

[12] 17 C.F.R § 248.201 (2013).
[13] *Id*.

33. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[14]

34. Identity thieves can use personal information, such as that of Plaintiffs and Class members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

35. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[15]

36. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[16]

37. There may be a time lag between when harm occurs versus when it is discovered, and also between when customer data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As

---

[14] Federal Trade Commission, *Warning Signs of Identity Theft, available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 30, 2019).

[15] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited July 30, 2019).

[16] Victims of Identity Theft, 2014 (Sept. 2015) *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 30, 2019).

a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

**B. Defendants' Representations Regarding Data Security**

38. During the credit card application process, Defendants make numerous representations to consumers regarding Defendants' purported efforts in safeguarding consumers' Customer Data.

39. At the top of Defendants' credit card application webpage, Defendants provide a bolded, clickable "Security" button which informs consumers that "when you are on our website, the data transferred between Capital One and you is encrypted and cannot be viewed by any other party."

40. Defendants' credit card application page also directs users to a "Privacy" page. Through the Privacy page, Defendants direct consumers to numerous representations regarding their Customer Data security measures, including the following: "[i]f we collect identifying information from you, *we will protect* that information with controls based upon internationally recognized security standards, ***regulations***, and industry-based best practices."

41. The Privacy page also directs consumers to Defendants' representation that "Capital One protects your Social Security Number" and that their "policies and procedures: 1. Protect the confidentiality of Social Security numbers; 2. Prohibit the unlawful disclosure of Social Security numbers; and 3. Limit access to Social Security numbers to employees or others with legitimate business purposes."

**C. Defendants Had Notice of Data Breaches**

42. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the highly sensitive Customer Data and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on their customers as a result of a breach.

43. Defendants explicitly recognized these risks in their Annual Information Forms leading up to and during the Data Breach. For example, as Defendants admitted in their 2018 Annual Information Form: "[a] ***disruption or breach***, including as a result of a ***cyber-attack***, or media reports

[17] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited July 30, 2019).

of perceived security vulnerabilities at Capital One or at third-party service providers, could result in significant legal and financial exposure, regulatory intervention, ***remediation costs***, card reissuance, supervisory liability, damage to our reputation or loss of confidence in the security of our systems, products and services that could adversely affect our business. ***We and other U.S. financial services providers continue to be targeted with evolving and adaptive cybersecurity threats from sophisticated third parties***."[18]

44. Moreover, Defendants were on notice of these types of data security incidents. Furthermore, a significant number of the data breaches in the past few years have targeted financial services and banking companies such as data breaches affecting Equifax, Heartland, JP Morgan Chase, and CitiFinancial.

45. In 2017, the number of U.S. data breaches was approximately 1,300, and the 2019 number is expected to surpass this.[19]

46. Despite the warnings and the acknowledgment of the risk, Defendants' approach to maintaining the privacy and security of the Plaintiffs' and Class members' Consumer Data was lackadaisical, cavalier, reckless, or at the very least, negligent.

47. For these reasons, Defendants disregarded Plaintiffs' and members of the Classes' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable data-security measures to ensure their data was protected, failing to take available steps to prevent and stop the breach from ever happening, failing to monitor and detect the breach on a timely basis, and failing to disclose to their customers the material facts that they did not have adequate security systems and practices to safeguard Customer Data.

**D. <u>Defendants Failed to Comply With FTC Requirements</u>**

48. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial

---

[18] Capital One Financial Corporation., Annual Information Sheet, at 24 http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-reportsannual (last visited July 30, 2019).

[19] https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78 (last visited July 30, 2019).

institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[21] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC also recommends that companies limit access to sensitive data, require complex and secure passwords to be used on networks, require authentication, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[20] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwith security.pdf (last visited July 30, 2019).

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 30, 2019).

[22] Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwith security.pdf (last visited July 30, 2019).

52. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

53. In this case, Defendants were at all times fully aware of their obligation to protect the private data of their customers. Defendants were also aware of the significant repercussions if they failed to do so because Defendants collects private information from millions of customers and they knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

54. Despite understanding the consequences of inadequate data security, Defendants failed to comply with FTC requirements, including but not limited to failing to properly dispose of personal information that is no longer needed, as Defendants stored Customer Data since 2005. Defendants further failed to take additional protective measures beyond those required by FTC.

## CLASS ALLEGATIONS

55. Plaintiffs seek relief on behalf of themselves and as the representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), Plaintiffs seek to certify a class of all persons residing in the United States who applied for any of Defendants' credit cards since 2005 (the "Nationwide Class").

56. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Belinda Fisher also seeks to certify a class of all persons residing in Oregon who applied for any of Defendants' credit cards since 2005 (the "Oregon Subclass").

57. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Stevens and Thaxton also seek to certify a class of all persons residing in Washington who applied for any of Defendants' credit cards since 2005 (the "Washington Subclass").

58. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Clark also seeks to certify a class of all persons residing in California who applied for any of Defendants' credit cards since 2005 (the "California Subclass").

59. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Jewell also seeks to certify a class of all persons residing in Kansas who applied for any of Defendants' credit cards since 2005 (the "Kansas Subclass").

60. The Nationwide Class, Oregon Subclass, Washington Subclass, Kansas Subclass, and California Subclass are individually referred to as "Class" and collectively referred to as the "Classes."

61. The Oregon Subclass, Washington Subclass, Kansas Subclass, and the California Subclass are collectively referred to as the "State Subclasses."

62. Excluded from each of the Classes are Defendants and any of their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judges to whom this case is assigned as well as his or her judicial staff and immediate family members.

63. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

64. Plaintiff Fisher is a member of the Nationwide Class and the Oregon Subclass.

65. Plaintiff Clark is a member of the Nationwide Class and the California Subclass.

66. Plaintiffs Stevens and Thaxton are members of the Nationwide Class and the Washington Subclass.

67. Plaintiff Jewell is a member of the Nationwide Class and the Kansas Subclass.

68. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

69. **Numerosity.** The proposed Classes includes at least 100 million customers whose data was compromised in the breach. The massive size of the data breach indicates that joinder of each member would be impracticable.

70. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. Whether Defendants had a duty to protect the Customer Data;

b. Whether Defendants knew or should have known of the susceptibility of their data security to a data breach;

c. Whether Defendants' security measures to protect their data were reasonable in light of the FTC data security requirements, and other measures recommended by data security experts;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' failure to implement adequate data security measures allowed the data breach;

f. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of the Customer Data of Plaintiffs and Class members;

g. Whether Defendants' breaches of their legal duties caused Plaintiffs and the Class members to suffer damages;

h. Whether Plaintiffs and Class members are entitled to recover damages; and

i. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

71. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and Class members were injured through Defendants' uniform misconduct and their legal claims arise from the same core practices employed or omitted by Defendants.

72. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiffs are adequate representatives of the proposed Classes because their interests do not conflict with the interests of the Class members they seek to represent. Plaintiffs' counsel is experienced in litigating consumer class actions and complex commercial disputes, and include lawyers who have successfully prosecuted similarly massive data breach cases.

73. **Superiority. Fed. R. Civ. P. 23(a)(5).** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class

member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

74. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendants have acted or have refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

**COUNT I**
**Breach Of Implied Contract**
**(*On Behalf Of Plaintiffs And The Nationwide Class Or, Alternatively, Plaintiffs And The State Subclass*)**

75. Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth herein.

76. Defendants solicited and invited Plaintiffs and Class members to create or apply for credit cards and provide their Customer Data in order to do so. Plaintiffs and Class members accepted Defendants' offer and provided their Customer Data in doing so.

77. In so doing, Plaintiffs and Class members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their Customer Data.

78. Plaintiffs and Class members would not have provided and entrusted their Customer Data to Defendants in the absence of the implied contract between them and Defendants.

79. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

80. Defendants breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their Consumer Data and by failing to timely detect the data breach within a reasonable time.

81. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants and Plaintiffs and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

**COUNT II**
**Negligence**
**(*On Behalf Of Plaintiffs And The Nationwide Class Or, Alternatively, Plaintiffs And The State Subclass*)**

82. Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth herein.

83. Upon accepting and storing the Plaintiffs' and Class members' Customer Data in servers, Defendants undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Customer Data was private and confidential and should be protected as private and confidential.

84. Defendants owed a duty of care not to subject Plaintiffs' and Class members' Customer Data to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

85. Defendants owed numerous duties to Plaintiffs and Class members, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Customer Data in their possession;

b. to protect Customer Data using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

86. Defendants breached their duty to Plaintiffs and Class members to adequately protect and safeguard Customer Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to the Customer Data. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Customer Data with which they were and are entrusted, despite the known risk and foreseeable

likelihood of breach and misuse, which permitted a malicious third party to gather the Customer Data of Plaintiffs and Class members.

87. Defendants knew, or should have known, of the risks inherent in collecting and storing Customer Data and the importance of adequate security. Defendants knew or should have known about numerous, well-publicized data breaches within the financial services, retail, and e-commerce industries. Defendants even recognized this risk, explicitly stating that their systems "continue to be targeted" by cybersecurity threats.

88. Defendants knew, or should have known, that their data systems and servers did not adequately safeguard Plaintiffs' and Class Members' Customer Data.

89. Defendants were further negligent by holding onto Plaintiffs' and Class Members' Customer Data for approximately 2005, increasing the breadth and severity of the Data Breach.

90. Because Defendants knew that a breach of their systems and servers would damage millions of their customers, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and servers and the Customer Data contained thereon.

91. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendants with their Customer Data was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants have the ability to protect their systems and servers and the Customer Data they stored on them from attack.

92. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Customer Data.

93. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Customer Data. Defendants' misconduct included failing to: (1) secure their data security systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

94. Defendants also had independent duties under state and federal laws that required them to reasonably safeguard Plaintiffs' and Class members' Customer Data and promptly notify them about the data breach.

95. Defendants breached their duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Customer Data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' Customer Data;

d. failing to properly dispose of Customer Data that is no longer needed;

e. failing to comply with the minimum industry data security standards during the period of the Data Breach; and

f. by failing to discover the breach in a timely manner.

96. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Customer Data as described in this Complaint.

97. As a direct and proximate cause of Defendants' conduct, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from late fees charged and foregone cash back rewards; damages from lost money, time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage

and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

**COUNT III**
**Negligence *Per Se***
**(*On Behalf Of Plaintiffs And The Classes*)**

On Behalf of the California Subclass

98. Plaintiff Clark restates and realleges Paragraphs 1 through 74 as if fully set forth herein.

99. Section 1798.81.5(b) of the California Civil Code establishes that any "business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

100. Defendants violated Section 1798.81.5(b) of the California Civil Code by failing to implement and maintain reasonable security procedures and practices necessary to protect Plaintiff Clark's and Class members' private information from unauthorized access.

101. Defendants' violation of Section 1798.81.5(b) of the California Civil Code thereby constitutes negligence *per se*.

102. Plaintiff Clark and Class members are within the class of persons that California Civil Code Section 1798.81.5(b) was intended to protect because they are California residents.

103. The harm which occurred due to Defendants' Data Breach is the type of harm that California Civil Code Section 1798.81.5(b) was intended to protect. Specifically, this is the harm of the unauthorized access or disclosure of personal information due to a failure to maintain reasonable security procedures.

On Behalf of the Oregon Subclass

104. Plaintiff Fisher restates and realleges Paragraphs 1 through 74 as if fully set forth herein.

105. Or. Rev. Stat. § 646A.622(1) establishes that any businesses must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information.

106. Or. Rev. Stat. § 646A.604(1) further requires Defendants to disclose the data breach in a timely and accurate manner.

107. Defendants violated Or. Rev. Stat. § 646A.622(1) by failing to implement and maintain reasonable security procedures and practices necessary to protect Plaintiff Fisher's and Oregon Subclass members' Customer Data from unauthorized access.

108. Defendants violated Or. Rev. Stat. § 646A.604(1) by failing to disclose the data breach in a timely and accurate manner.

109. Plaintiff Fisher and Oregon Subclass members are within the class of persons that Or. Rev. Stat. § 646A.622(1) and Or. Rev. Stat. § 646A.604(1) were intended to protect because they are Oregon residents whose personal information was disclosed as a result of Defendants' Data Breach.

110. The harm which occurred due to Defendants' Data Breach is the type of harm that Or. Rev. Stat. § 646A.622(1) and Or. Rev. Stat. § 646A.604(1) were intended to protect. Specifically, this is the harm of the unauthorized access or disclosure of personal information due to a failure to maintain reasonable security procedures.

111. Defendants' violations of Or. Rev. Stat. § 646A.622(1) and Or. Rev. Stat. § 646A.604(1) thereby constitute negligence *per se*.

On Behalf of the Kansas Subclass

112. Plaintiff Jewell restates and realleges Paragraphs 1 through 74 as if fully set forth herein.

113. Kan. Stat. Ann. § 50-7a02(a) establishes that any businesses that owns or licensed computerized data, such as the Customer Data, must notify Kansas residents upon becoming aware of a breach of their data security system that was reasonably likely to have caused misuse of the data in the most expedient time possible and without unreasonable delay.

114. Defendants violated Kan. Stat. Ann. § 50-7a02(a) because Defendants were aware of a breach of their security system that was reasonably likely to have caused misuse of Plaintiff Jewell's and Kansas Subclass members' Customer Data, but failed to notify Plaintiff Jewell and Kansas Subclass members in the most expedient time possible and without unreasonable delay.

115. Plaintiff Jewell and Kansas Subclass members are within the class of persons that Or. Rev. Stat. § 646A.622(1) and Or. Rev. Stat. § 646A.604(1) were intended to protect because they are Kansas residents whose personal information was disclosed as a result of Defendants' Data Breach.

116. The harm which occurred due to Defendants' Data Breach is the type of harm that Kan. Stat. Ann. § 50-7a02(a) was intended to protect. Specifically, this is the harm of the delayed notification regarding Defendants' Data Breach to Plaintiff Jewell and Kansas Subclass members.

117. Defendants' violation of Kan. Stat. Ann. § 50-7a02(a) thereby constitutes negligence *per se*.

On Behalf of the Washington Subclass

118. Plaintiffs Thaxton and Stevens restate and reallege Paragraphs 1 through 74 as if fully set forth herein.

119. Wash. Rev. Code § 19.255.010(1) establishes that any businesses that own or license "personal information", such as the Customer Data, are required to accurately notify Washington residents following discovery or notification of any breaches of their data security system if "personal information" was, or is reasonably believed to have been, acquired by an unauthorized person and the "personal information" was not secured, in the most expedient time possible and without unreasonable delay.

120. Defendants violated Wash. Rev. Code § 19.255.010(1) Defendants discovered a cybersecurity breach of its data systems which stored the Customer Data that was or is reasonably believed to have been acquired by an authorized person and the Customer Data was not secured, but Defendants failed to disclose the data breach in a timely and accurate fashion as mandated.

121. Plaintiffs Thaxton and Stevens and Washington Subclass members are within the class of persons Wash. Rev. Code § 19.255.010 was intended to protect because they are Washington residents whose personal information was disclosed as a result of Defendants' Data Breach.

122. The harm which occurred due to Defendants' Data Breach is the type of harm that Wash. Rev. Code § 19.255.010(1) was intended to protect. Specifically, this is the harm of the delayed notification regarding Defendants' Data Breach to Plaintiffs Thaxton and Stevens and Washington Subclass members.

123. Defendants' violation of Wash. Rev. Code § 19.255.010(1) thereby constitutes negligence *per se*.

On Behalf of the Classes

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Customer Data. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

125. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Customer Data as described in detail herein, including but not limited to failing to properly dispose of Customer Data that is no longer needed. Defendants' conduct was particularly unreasonable given the nature and amount of Customer Data they obtained and stored, including, specifically, the immense damages that would result to Plaintiffs and Class members.

126. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

127. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the Defendants' Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

129. As a direct and proximate cause of Defendants' conduct, Plaintiffs and the Class members suffered damages including, but not limited to: damages arising from late fees charged and foregone cash back rewards; damages from lost money, time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

**COUNT IV**
**Unjust Enrichment**
**(*On Behalf Of Plaintiffs And The Nationwide Class Or, Alternatively, Plaintiffs And The State Subclasses*)**

130. Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth here.

131. Plaintiffs and Class members conferred a benefit on Defendants. Specifically, they applied for credit cards and provided Defendants with their Customer Data and payment information. In exchange, Plaintiffs and Class members should have been entitled to have Defendants protect their Customer Data with adequate data security.

132. Defendants knew that Plaintiffs and Class members conferred a benefit on them and has accepted or retained that benefit. Defendants profited from the credit card applications and used Plaintiffs' and Class members' Customer Data for business purposes.

133. Defendants failed to secure Plaintiffs' and Class members' Customer Data and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' Customer Data provided.

134. Defendants acquired the Customer Data through inequitable means as they failed to disclose the inadequate security practices previously alleged.

135. If Plaintiffs and Class members knew that Defendants would not secure their Customer Data using adequate security, they would not have applied for the credit cards and provided Defendants with their data.

136. Plaintiffs and Class members have no adequate remedy at law.

137. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on it.

138. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

**COUNT V**
**Declaratory Judgment**
**(*On Behalf Of Plaintiffs And The Nationwide Class Or, Alternatively, Plaintiffs And The State Subclasses*)**

139. Plaintiffs restate and reallege Paragraphs 1 through 74 as if fully set forth here.

140. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

141. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Defendants to provide adequate security for the Customer Data they collected from their applying for credit cards from Defendants. As previously alleged, Defendants owes duties of care to Plaintiffs and Class members that require them to adequately secure that Customer Data.

142. Defendants still possesses Customer Data pertaining to Plaintiffs and Class members.

143. Accordingly, Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Defendants' lax approach towards data security has become public, the Customer Data in their possession is more vulnerable than previously.

144. Actual harm has arisen in the wake of the Defendants Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

145. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

i. Defendants continues to owe a legal duty to secure consumers' Customer Data and to timely and accurately notify consumers of the data breach under California law, common law, and Section 5 of the FTC Act;

j. Defendants' existing data security measures do not comply with their legal duties of care; and

k. Defendants continues to breach their legal duty by failing to employ reasonable measures to secure consumers' Customer Data.

146. Plaintiffs also requests an injunction requiring Defendants to comply with their contractual obligations and duties of care and implement and maintain reasonable security measures, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems and servers periodically, and ordering Defendants to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement[ing] and maintain[ing] reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training their security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of stronger firewalls and access controls so that if one area of Defendants' data security measures are compromised, hackers cannot gain access to other areas of Defendants' systems;

f. deleting, in a reasonable and secure manner, Customer Data not necessary for Defendants' provisions of goods or services;

g. conducting regular database scanning and security checks;

h. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

i. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

147. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event Defendants incurs another data breach. The risk of another such breach is real, immediate, and substantial.

148. The hardship to Plaintiffs and other customers if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. If Defendants incurs another data breach, Plaintiffs and other customers will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

149. Such an injunction would benefit the public by preventing another data breach for Defendants, and therefore eliminating the additional injuries that would result to Plaintiffs and the millions of customers whose confidential information would be further compromised.

**COUNT VI**
**Violation Of California Consumer Privacy Act**
**Cal. Civ. Code § 1798.81.5**

**(*On Behalf Of Plaintiff Clark And The California Subclass*)**

150. Plaintiff Clark restates and realleges paragraphs 1 through 74 above as if fully set forth herein.

151. Cal Civ. Code § 1798.81.5(a)(1) provides that its purpose is to "ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

152. Cal. Civ. Code § 1798.81.5(b) provides, in pertinent part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

153. Under Cal Civ. Code § 1798.81.5(d)(1), "personal information" includes names, social security numbers, and account numbers.

154. Therefore, some of the Customer Data stolen in the Defendants' Data Breach falls within the meaning of "personal information" under Cal. Civ. Code Section 1798.81.5.

155. By failing to implement adequate and reasonable data security measures for this Customer Data, Defendants violated Cal. Civ. Code Section 1798.81.5.

156. Because Defendants violated Cal. Civ. Code Sections 1798.81.5, Plaintiff Clark may seek an injunction pursuant to Cal. Civ. Code Section 1798.84(e), which states "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Specifically, Plaintiff Clark seeks injunctive relief requiring Defendants to implement and maintain adequate and reasonable data security measures and abide by the California Data Breach laws, including, but not limited to:

a. hiring third-party security auditors and penetration testers in addition to internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems periodically, and ordering Defendants to promptly rectify any flaws or issues detected by such parties;

b. as required by Cal. Civ. Code Section 1798.81.5, "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.";

c. engaging third-party security auditors and internal personnel to run automated security monitoring;

d. testing, auditing, and training their security personnel regarding any and all new and/or modified security measures or procedures;

e. creating further and separate protections for customer data including, but not limited to, the creation of firewalls and access controls so that if one area of Defendants' data security measures are compromised, hackers cannot gain access to other areas of Defendants' systems;

f. utilizing more complex and multilayered authentication;

g. requiring consumers use more complex and unique passwords;

h. warning consumers of the substantial risks and effects of credential stuffing, instructing affected consumers to change their credentials on other e-commerce and web platforms they use.

i. deleting, in a reasonable and secure manner, Customer Data not necessary for Defendants' provisions of products or services;

j. conducting regular database scanning and security checks;

k. conducting routine and periodic training and education to prepare internal security personnel regarding the processes to identify and contain a breach when it occurs and what appropriate actions are proper in response to a breach; and

l. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

**COUNT VII**
**Violation Of California's Unfair Competition Law ("UCL"),**
**California Business & Professions Code §§ 17200, *et seq.***
**(*On Behalf Of Plaintiff Clark And The California Subclass*)**

157. Plaintiff Clark restates and realleges Paragraphs 1 through 74 above as if fully set forth herein.

158. UCL § 17200 provides, in pertinent part, that "unfair competition shall mean and include unlawful, unfair, or fraudulent business practices [. . .]"

159. Under the UCL, a business act or practice is "unlawful" if the act or practice violates any established state or federal law.

160. Defendants' failures to implement and maintain reasonable security measures and to timely and properly notify Plaintiff Clark and California Subclass members of the Data Breach therefore was and continues to be "unlawful" as Defendants breached their implied warranties and violated the California laws regarding data breaches, including California Civil Code §§ 1798.81.5, as well as the FTC Act.

161. As a result of Defendants' unlawful business acts and practices, Defendants unlawfully obtained money from Plaintiff Clark and members of the California Subclass.

162. Under the UCL, a business act or practice is "unfair" if the Defendants' conduct is substantially injurious to consumers, goes against public policy, and is immoral, unethical, oppressive, and unscrupulous, as the benefits for committing these acts or practices are outweighed by the severity of the harm to the alleged victims.

163. Here, Defendants' reckless conduct was and continues to be of no benefit to their customers, as it is both injurious and unlawful to those persons who rely on Defendants' duties and obligations to maintain and implement reasonable data security measures and to monitor for breaches. Having lax data security measures that has resulted in the disclosure of millions of customers' payment card information provides no benefit to consumers. For these reasons, Defendants' conduct was and continues to be "unfair" under the UCL.

164. As a result of Defendants' unfair business acts and practices, Defendants have unfairly and unlawfully obtained money from Plaintiff Clark and members of the California Subclass.

165. Plaintiff Clark requests that this Court enjoin Defendants from violating the UCL or violating the UCL in the same way in the future, as discussed herein. Otherwise, Plaintiff Clark and members of the California Subclass may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

**COUNT VIII**
**Violation Of Oregon Consumer Information Protection Act**
**Or. Rev. Stat. §§ 646A.604(1), *et seq*.**
**(*On Behalf Of Plaintiff Fisher and the Oregon Subclass*)**

166. Plaintiff Belinda L. Fisher restates and reallege Paragraphs 1 through 74 above as if fully set forth herein.

167. Defendants have violated Or. Rev. Stat. § 646A.622(1) by failing to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information given to them by Plaintiff Fisher and the Oregon Subclass members, as described above.

168. Defendants have also violated Or. Rev. Stat. § 646A.604(1) by failing to disclose the data breach in a timely and accurate manner.

169. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

170. As a direct and proximate result of Defendants' violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff Fisher and Oregon Subclass members suffered damages, as described above.

171. Plaintiff Fisher and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

**COUNT IX**
**Violation Of Oregon Unlawful Trade Practices Act**
**Or. Rev. Stat. §§ 646.608, *et seq*.**
**(*On Behalf Of Plaintiffs Belinda L. Fisher and the Oregon Subclass*)**

172. Plaintiff Fisher restate and reallege Paragraphs 1 through 74 above as if fully set forth herein.

173. Defendants are "persons" as defined by Or. Rev. Stat. § 646.605(4).

174. Defendants' conduct as alleged herein pertained to "goods" and "services" as defined by Or. Rev. Stat. § 646.605(6)(a).

175. Defendants advertised, offered, and sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the citizens of Oregon.

176. Defendants engaged in the following unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608:

a. Representing that their goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that their goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising their goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i);

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

177. Defendants' unlawful practices include:

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Fisher and Oregon Subclass members' Customer Data, which was a direct and proximate cause of the data breach;

f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Fisher and Oregon Subclass members' Customer Data, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Or. Rev. Stat. §§

646A.600, *et seq*., which was a direct and proximate cause of the data breach;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Fisher and Oregon Subclass members' Customer Data, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Fisher and Oregon Subclass members' Customer Data, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Or. Rev. Stat. §§ 646A.600, *et seq*.;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Fisher and Oregon Subclass members' Customer Data;

k. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Fisher and Oregon Subclass members' Customer Data, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Or. Rev. Stat. §§ 646A.600, *et seq*.

178. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Customer Data.

179. Defendants intended to mislead Plaintiff Fisher and Oregon Subclass members and induce them to rely on their misrepresentations and omissions.

180. Had Defendants disclosed to Plaintiff Fisher and Class members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable Customer regarding millions of consumers, including Plaintiff Fisher and the Oregon Subclass. Accordingly, Plaintiff Fisher and the Oregon Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

181. Defendants acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff Fisher and Oregon Subclass members' rights. Defendants' past data breach, as well as those affecting other financial service companies and retailers, put Defendants on notice that their security and privacy protections were inadequate.

182. As a direct and proximate result of Defendants' unlawful practices, Plaintiff Fisher and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Customer Data.

183. Plaintiff Fisher and Oregon Subclass members seek all monetary and nonmonetary relief allowed by law, including equitable relief, actual damages or statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

**COUNT X**
**Violation Of Kansas Protection of Consumer Information Act**
**Kan. Stat. Ann. §§ 50-7a02(a), *et seq.***
**(*On Behalf Of Plaintiff Jewell and the Kansas Subclass*)**

184. Plaintiff Jewell restates and realleges Paragraphs 1 through 74 above as if fully set forth herein.

185. Defendants are businesses that own or license computerized data that includes Customer Data as defined by Kan. Stat. Ann. § 50-7a02(a).

186. Plaintiff Jewell's and Kansas Subclass members' Customer Data (*e.g.*, Social Security numbers and financial account numbers) includes Customer Data as covered under Kan. Stat. Ann. § 50-7a01(g).

187. Defendants are required to accurately notify Plaintiff Jewell and Kansas Subclass members when they become aware of a breach of their data security system that was reasonably likely to have caused misuse of Plaintiff Jewell's and Kansas Subclass members' Customer Data, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

188. Because Defendants were aware of a breach of their security system that was reasonably likely to have caused misuse of Plaintiff Jewell's and Kansas Subclass members' Customer Data, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50- 7a02(a).

189. By failing to disclose the data breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

190. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff Jewell and Kansas Subclass members suffered damages, as described above. Plaintiff Jewell and Kansas Subclass members therefore seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

**COUNT XI**
**Violation Of Kansas Consumer Protection Act**
**Kan. Stat. Ann. §§ 50-623, *et seq.***
**(*On Behalf Of Plaintiff Jewell and the Kansas Subclass*)**

191. Plaintiff Jewell restates and realleges Paragraphs 1 through 74 above as if fully set forth herein.

192. Kan. Stat. Ann. §§ 50-623 is to be liberally construed in order to protect consumers from suppliers who engage in deceptive and unconscionable practices.

193. Plaintiff Jewel and members of the Kansas Subclass are "consumers" within the meaning of Kan. Stat. Ann. §§ 50-624(b).

194. Defendants' acts and practices as alleged herein are "consumer transactions" within the meaning of Kan. Stat. Ann. §§ 50-624(c).

195. Defendants are "suppliers" within the meaning of Kan. Stat. Ann. §§ 50-624(1).

196. Defendants advertised, sold, and offered goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

197. Based on the allegations herein, Defendants engaged in deceptive and unfair acts or practices, including the following:

a. Failing to implement and maintain adequate and reasonable data security measures to

protect Plaintiff Jewell and the Kansas Subclass members' Customer Data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, fix identified security and privacy risks, and properly improve Defendants' data security measures to adequately identify, prevent cybersecurity attacks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with duties imposed by common law and statutes relating to safeguarding Plaintiff Jewell and the Kansas Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45 and the Kansas Protection of Consumer Information Act, Kan. Stat. Ann., §§ 50-7a02(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would adequately safeguard Plaintiff Jewell's and Kansas Subclass members' Customer Data, including by implementing adequate safeguards and protections for the data;

e. Misrepresenting that Defendants would comply with duties imposed by common law and statutes relating to safeguarding Plaintiff Jewell and Kansas Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45 and the Kansas Protection of Consumer Information Act, Kan. Stat. Ann., §§ 50-7a02(a), which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Jewell and Kansas Subclass members' Customer Data; and

g. Omitting, suppressing, and concealing the material fact that Defendants failed to comply with duties imposed by common law and statutes relating to safeguarding Plaintiff Jewell and Kansas Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45 and the Kansas Protection of Consumer Information Act Kan. Stat. Ann., §§ 50-7a02(a), which was a direct and proximate cause of the Data Breach.

198. In making their misrepresentations and omissions, Defendants intended to mislead and

induce Plaintiff Jewell and Kansas Subclass members into relying on them.

199. Defendants' omissions and misrepresentations were material because they were the type to deceive reasonable consumers regarding the adequacy of Defendants' data security measures and Defendants' ability to adequately protect the Customer Data from cyberattacks.

200. If Defendants disclosed to Plaintiff Jewell and Kansas Subclass Members that Defendants' data security measures were inadequate and insecure, Plaintiff Jewell and Kansas Subclass members would have refrained from purchasing goods or services from Defendants and Defendants would have been unable to continue its normal business operations, forcing Defendants to improve their data security measures until they were adequate and in compliance with any common law and statutory duties. Instead, Defendants represented that their data security measures were adequate and omitted the vulnerabilities of these data security measures. Because Defendants took this position, Plaintiff Jewell and Kansas Subclass members reasonably relied on Defendants' misrepresentations and omissions, reasonably believing that Defendants' data security measures were adequate. There was no way for Plaintiff Jewell or Kansas Subclass members to reasonably discover that Defendants' data security measures were inadequate.

201. Defendants' conduct alleged herein also constituted unconscionable conduct in violation of K.S.A. § 50-627, including:

a. Defendants knowingly took advantage of Plaintiff Jewell and Kansas Subclass members' lack of knowledge land inability to reasonable protect their interests in violation of K.S.A. § 50-627(b)(1); and

b. Knowingly inducing Plaintiff Jewell and Kansas Subclass members to enter into an agreement which was excessively one-sided in favor of Defendants in violation of K.S.A. § 50-627(b)(5).

202. Plaintiff Jewell and the Kansas Subclass members had unequal bargaining power in regard to their ability to control the security and confidentiality of their Customer Data in Defendants' possession and control.

203. Defendants' aforementioned conduct was immoral, unethical, oppressive, and

unscrupulous. These unfair, deceptive, and unconscionable practices and acts caused substantial injury to Plaintiff Jewell and Kansas Subclass members which they could not have reasonably avoided. These injuries were outweighed by any potential benefits to consumer or to competition.

204. Defendants acted intentionally, knowingly, and maliciously when violating Kansas' consumer protection statute, and in doing so, recklessly disregarded the rights of Plaintiff Jewell and Kansas Subclass members. Previous data breaches in the industry, including Defendants' past admissions that the Customer Data was vulnerable and "continue to be targeted" by attacks put Defendants on notice that its data security measures and protections were inadequate.

205. Plaintiff Jewell and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages, in the greater amount, under K.S.A. §§ 509-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT XII**
**Violation of Washington's Data Breach Notice Act**
**Wash. Rev. Code §§ 19.255.010, *et seq.***
**(*On Behalf Of Plaintiffs Thaxton, Stevens, and the Washington Subclass*)**

206. Plaintiffs Thaxton and Stevens restate and reallege Paragraphs 1 through 74 above as if fully set forth herein.

207. Defendants are businesses that own or license computerized data, including the Customer Data, within the meaning of Wash. Rev. Code § 19.255.010(1).

208. Plaintiffs Thaxton's and Stevens' and members of the Washington Subclass' Customer Data includes "personal information" within the meaning of Wash. Rev. Code § 19.255.010(5).

209. Defendants are required to accurately notify Plaintiffs Thaxton and Stevens and members of the Washington Subclass following discovery or notification of any breaches of their data security system if "personal information" within the meaning of Wash. Rev. Code § 19.255.010(5), which includes the Customer Data, was, or is reasonably believed to have been, acquired by an unauthorized person and the "personal information" was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

210. Because Defendants discovered a cybersecurity breach of its data systems which stored the Customer Data, containing "personal information" within the meaning of Wash. Rev. Code § 19.255.010(5), was or is reasonably believed to have been acquired by an authorized person and the Customer Data was not secured, Defendants had a duty to disclose the data breach in a timely and accurate fashion as mandated Wash. Rev. Code § 19.255.010(1).

211. Because Defendants failed to disclose the Data Breach in a timely and accurate fashion, Defendants violated Wash. Rev. Code § 19.255.010(1).

212. As a direct and proximate result of Defendants' violation of Wash. Rev. Code § 19.255.010(1), Plaintiffs Thaxton and Stevens, and members of the Washington Subclass, suffered damages as described above.

213. Plaintiffs Thaxton and Stevens, and members of the Washington Subclass, seek relief under Wash. Rev. Code § 19.255.013(a) and Wash. Rev. Code § 19.255.013(b).

**COUNT XIII**
**Violation of Washington's Consumer Protection Act**
**Wash. Rev. Code §§ 19.86.020, *et seq.***
**(*On Behalf Of Plaintiffs Thaxton, Stevens, and the Washington Subclass*)**

214. Plaintiffs Thaxton and Stevens restate and reallege Paragraphs 1 through 74 above as if fully set forth herein.

215. Defendants are "persons" within the meaning of Wash. Rev. Code § 19.86.010(1).

216. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington within the meaning of Wash. Rev. Code § 19.86.010(2).

217. Defendants engaged in unfair and deceptive acts and practices while engaging in trade or commerce in violation of Wash. Rev. Code § 19.86.020 by:

a. Failing to implement and maintain adequate and reasonable data security measures to protect Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, fix identified security and privacy risks, and properly improve Defendants' data security measures to adequately

identify, prevent cybersecurity attacks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with duties imposed by common law and statutes relating to safeguarding Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45, and Washington's Data Breach Notice Act Wash. Rev. Code §§ 19.255.010, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would adequately safeguard Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data, including by implementing adequate safeguards and protections for the data;

e. Misrepresenting that Defendants would comply with duties imposed by common law and statutes relating to safeguarding Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45, and Washington's Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, *et seq.*, which was a direct and proximate cause of the Data Breach;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data; and

g. Omitting, suppressing, and concealing the material fact that Defendants failed to comply with duties imposed by common law and statutes relating to safeguarding Plaintiffs Thaxton' and Stevens' and Washington Subclass members' Customer Data, including those imposed by the FTC Act, 15 U.S.C. § 45, and Washington's Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, *et seq.*, which was a direct and proximate cause of the Data Breach.

218. In making their misrepresentations and omissions, Defendants intended to mislead and induce Plaintiffs Thaxton and Stevens and Washington Subclass members into relying on them.

219. Defendants' omissions and misrepresentations were material because they were the

type to deceive reasonable consumers regarding the adequacy of Defendants' data security measures and Defendants' ability to adequately protect the Customer Data from cyberattacks.

220. Defendants acted intentionally, knowing, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiffs Thaxton' and Stevens' and Washington Subclass members' rights. Previous data breaches in the industry, including Defendants' past admissions that the Customer Data was vulnerable and "continue to be targeted" by attacks put Defendants on notice that its data security measures and protections were inadequate.

221. Defendants' conduct is also injurious to the public interest because it violates Wash. Rev. Code § 19.86.020, a statute with a specific legislative declaration of public interest impact that has the capacity to injure Washington consumers. Additionally, Defendants' conduct affected the public interest, including numerous Washington residents affected by the Data Breach.

222. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, including their unfair methods of competition, Plaintiffs Thaxton and Stevens, and Washington Subclass members, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Customer Data.

223. Plaintiffs Thaxton and Stevens, and members of the Washington Subclass, seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

## REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendants as follows:

a) For an order certifying the Nationwide Class and the State Subclasses under Rule 23 of the Federal Rules of Civil Procedure; naming Plaintiffs as representative of all Classes; and naming Plaintiffs' attorneys as Class Counsel to represent all Classes;

b) For an order declaring that Defendants' conduct violates the statutes and laws

referenced herein;

c) For an order finding in favor of Plaintiffs, and all Classes, on all counts asserted herein;

d) For an order awarding all damages in amounts to be determined by the Court and/or jury;

e) For prejudgment interest on all amounts awarded;

f) For interest on the amount of any and all economic losses, at the prevailing legal rate;

g) For an order of restitution and all other forms of equitable monetary relief;

h) For injunctive relief as pleaded or as the Court may deem proper;

i) For an order awarding Plaintiffs and all Classes their reasonable attorneys' fees, expenses and costs of suit, including as provided by statute such as under the Federal Rules of Civil Procedure 23(h); and

j) For any other such relief as the Court deems just and proper.

**DEMAND FOR TRIAL BY JURY**

Plaintiffs demand a trial by jury on all issues so triable.

Dated: August 1, 2019

**FARUQI & FARUQI, LLP**

By: */s/ Benjamin Heikali*
Benjamin Heikali, Bar No. 307466
Joshua Nassir, Bar No. 318344
10866 Wilshire Blvd., Suite 1470
Los Angeles, CA 90024
Telephone: 424.256.2884
Fax: 424.256.2885
E-mail: bheikali@faruqilaw.com
E-mail: jnassir@faruqilaw.com

**WALSH PLLC**

Bonner C. Walsh (*pro hac vice forthcoming*)
1561 Long Haul Road
Grangeville, ID 83530

Telephone: (541) 359-2827
Facsimile: (866) 503-8206
Email: bonner@walshpllc.com